CS3600 – Winter AY03
Reading Assignments by Section

Section	Topic	Information Warfare and Security
1	Introduction	Chap 1 Chap 3
2	I & A DAC	Chap 8, pp 203-214 Chap 12, pp 321-329 Chap 12, pp 340-344
3	MAC	Chap 13, pp 345-349
4	Design and Implementation Issues	Chap 13, pp 349-352
5	Malicious Software	Chap 8, pp 214-219 Chap 9, pp 258-265 Chap 10
6	System Accreditations and Evaluations	Chap 14, pp 375-382 Chap 14, pp 385-390
7	Cryptography Basics	Chap 11, pp 285-303 Chap 12, pp 329-331
8	Cryptographic Protocols	Chap 12, pp 331-335
9	Networks I, Basics	Chap 11, pp 306-313
10	Networks II, TCP, Firewalls, Intrusion Detection	Chap 7, pp 184-185 Chap 8, pp 234-239 Chap 9, pp 247-256 Chap 13, pp 352-369
11	Networks III, Public Key Infrastructure	Chap 11, pp 303-305 Chap 12, pp 336-338

Reading Questions

Book: Information Warfare and Security

There are some topics in the reading assignments that are not covered in class in any detail, or not at all. The questions that are listed in the following pages emphasize those parts of the reading assignments that we have not discussed in class, but which I consider important to remember.

Section 1
Introduction

Chapter 1

1. The author makes the statement: "100% security is neither possible nor worth the price." If 100% computer security is not possible, then what is the goal?
2. How much money does the author say it would take to fund a "highly paid information warfare team of 10 to 20 hackers"? Why is this a concern?

Chapter 3

3. Describe the likely characteristics (including the age) of the average hacker.
4. According to a survey by the American Society of Industrial Security (ASIS), which groups of people provide the highest risk for stealing corporate trade secrets?
5. Study the figures on pages 57 and 58. Figure 3.1 shows the kinds of attacks the surveyed companies detected. Figure 3.2 shows the financial loses associated which each kind of attack. If you were in charge of computer security, how can these figures help you to prioritize your efforts?

Section 2
Access Control I

Chapter 8 (pp. 203-214)

1. According to the author, if a hacker has gained access to a regular user account on a system, how hard is it to elevate his access to a more privileged account?
2. A 1997 survey conducted by Compaq found that 82% of users in the London financial district used "poor passwords" [assuming the environment was one where there were no proactive enforcement in place]. Given the kind of passwords they found, what kind of information would you need to know about someone in this kind of environment in order to have a good chance to guess their password?

Chapter 12 (pp. 321-329)

3. Why is Iris recognition considered very promising?
4. What is the attraction of voice recognition?

Chapter 12 (pp. 340-344)

5. Location-based authentication is a popular research area, especially with wireless networking. Describe two drawbacks that this approach might have?

Section 3
Access Control II

Chapter 13 (pp. 345-349)

1. How can many computer attacks be defeated?
2. What benefit would the enforcement of the "principle of least privilege" provide in a computer system?

Section 4
Building Secure Systems

Chapter 13 (pp. 349-352)

1. What can happen if computer access controls are not carefully designed and implemented?
2. The author lists six limitations to access control systems. Of the six, which ones are not a limitation of the design or implementation of access control products?

Section 5
Malicious Software and Attacks

Chapter 8 (pp. 214-219)

1. What were the two most common Internet vulnerabilities in 1997, as reported by Steve Bellovin. [One of these two is certainly still the most common vulnerability, and maybe always will be.]

Chapter 9 (pp. 258-265)

2. What is a "logic bomb"?

Chapter 10

3. Note that the term "Cyberplague" might be something she made up, but it's use has gained in popularity since the publication of the book.
4. What is the difference between a virus and a worm?
5. What do the majority of viruses do?
6. What seems to be the motivation for those who write viruses?
7. In your opinion, are there any security ramifications to virus hoaxes? Why?

Section 6
System Certification, Accreditation, and Evaluation

Chapter 14 (pp. 375-381)

1. In the opinion of the author, what were the limitations of the Orange Book?
2. Critical thinking: The Common Criteria is now recognized by many countries. Why was the trend toward every country having their own standard a bad thing?
3. Note: the author lists three potential limitations for ICSA Certification. These in fact apply to all evaluations and certifications, such as the Orange Book and the Common Criteria

Chapter 14 (pp. 385-390)

4. Why is risk assessment (risk analysis) not an exact science?
5. What three areas affect the value placed on information?

Section 7
Basics of Cryptography

Chapter 11 (pp. 285-305)

1. Theoretically, how many ciphers are breakable by brute force (given enough time)?
2. What are the first three things (in order) that must be determined when attempting to break an encrypted message?
3. Given the current increase in computing power, how long does the author say it will take before we have the computing power to reasonably do brute force on a 128-bit key?
4. Assume an encryption algorithm is embedded in an application. Also assume that the only known attack against the cipher is brute force, and its key is very long. What might still happen to allow the encryption to be broken in a reasonable amount of time?
5. What four things does “key management” include?
6. What is the Diffie-Helman protocol used for?
7. What are the advantages and disadvantages that elliptic curve cryptography have when compared to RSA?

Chapter 12 (pp. 329-331)

8. What is the advantage of using a hashing function that requires a key?

Section 8
Cryptographic Protocols

Chapter 12 (pp. 331-335)

1. What were the two “significant innovations” that public-key cryptography brought?

Section 9
Network Security I

Chapter 11 (pp. 306-313)

1. According to the data provided by the author, how much can a VPN save a company if it switched from private leased lines?
2. The use of Secure Socket Layer (SSL) does provide protection for the transmission of credit card numbers between a customer's system and a vendor's system. However, where can the credit card number still be vulnerable?
3. What are the two limitations of encryption given by the author?

Section 10
Network Security II

Chapter 7 (pp. 184-185)

1. What use are packet sniffers to an opponent?
2. What use are packet sniffers to the defenders?

Chapter 8 (pp. 234-239)

3. Describe SYN flooding and its affect on a target system.

Chapter 9 (pp 247-256)

4. What are the two ways to forge e-mail that were described by the author?
5. What is an e-mail bomb?

Chapter 13 (pp. 352-369)

6. What other functions can a firewall do besides those typically associated with a firewall?
7. What is the big potential drawback with all attempts to filter junk e-mail (spam)?
8. Critical Thinking: How does the filtering of spam relate to virus scanning? What general conclusion can be drawn about filtering?

Section 11
Public Key Infrastructure

Chapter 11 (pp. 303-305)

1. Describe some situations where a key recovery system would be beneficial.

Chapter 12 (pp. 336-338)

2. What is the difference between VeriSign's Class 1 and Class 2 public-key certificates?
3. Besides the challenging technical and managerial issues of developing a PKI, what other challenge(s) exist?